4

⑲日本国特許庁(JP)　⑪特許出願公告

⑫特許公報(B2)　平5−67980

| ⑤Int.Cl.⁵ | 識別記号 | 庁内整理番号 | | ㉔㊹公告 平成5年(1993)9月28日 |
|---|---|---|---|---|
| G 06 F 15/30 | 340 | 6798−5L | | |
| | 350 | 6798−5L | | |
| G 06 K 17/00 | S | 7459−5L | | |
| G 07 F 7/12 | | | | |
| G 09 C 1/00 | | 9194−5L | | |
| | | 7130−3E | G 07 F 7/08 | B |

発明の数 2 (全5頁)

㊹発明の名称　ICカードによる個人の認証方法

㉑特　願　昭59−1250　　㊺公　開　昭60−146361

㉒出　願　昭59(1984)1月10日　　㊸昭60(1985)8月2日

㉒発明者　家木　俊温　神奈川県横須賀市武1丁目2356番地　日本電信電話公社横須賀電気通信研究所内

㉑出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号

㉔代理人　弁理士　小林　将高　外1名

㉑出願人　エヌ・テイ・テイ・データ通信株式会社　東京都港区虎ノ門1丁目26番5号

㉔代理人　弁理士　小林　将高

審査官　森　繁明

㊻参考文献　特開　昭48−74150(JP,A)

1

㊼特許請求の範囲

1　個人が秘密保護を必要とするデータを暗号化してオンラインで相手側に送信する場合において、暗号化鍵とIDコードをICカード内のメモリにあらかじめ格納しておき、一方、IDコード発生関数と復号化鍵を相手側のセンタ内に設けておき、前記ICカードからカード番号が入力されたときこのコード番号を前記IDコード発生関数を通すことによりID′を算出し、一方、乱数であるパラメータαを前記ICカードへ送り、前記ICカードにおいてIDコードとパラメータαとから前記暗号化鍵によつて暗号文F(ID, α)を生成して前記相手側に送り、この相手側において前記暗号文F(ID, α)を前記復号化鍵に通してIDを算出し、前記ID′とIDとが一致したときのみ前記個人の認証を行うことを特徴とするICカードによる個人の認証方法。

2　個人が秘密保護を必要とするデータを暗号化してオンラインで相手側に送信し、相手が認証した後においてデイジタル署名を行う場合において、暗号化鍵、IDコードおよび署名関数Q(x)を

2

ICカード内のメモリにあらかじめ格納しておき、一方、IDコード発生関数，復化鍵および署名関数の発生関数P(x，y)を相手側のセンタ内に設けておき、前記ICカードからカード番号が入力されたときこのカード番号を前記IDコード発生関数を通すことによりID′を算出し、一方、乱数であるパラメータαを前記ICカードへ送り、前記ICカードにおいてIDコードとパラメータαとから前記暗号化鍵によつて暗号文F(ID, α)を生成して前記相手側に送り、この相手側において前記暗号文F(ID, α)を前記復号化鍵に通してIDを算出し、前記ID′とIDとが一致したときのみ前記個人の認証を行い、その後のデイジタル署名に際し、前記ICカードからカード番号を相手側に送り、相手側において前記カード番号を署名関数の発生関数P(x，y)に通して署名関数$Q^x(x)$を作成し、一方、乱数であるパラメータβを前記ICカードに送り、前記ICカード側は前記パラメータβを署名関数Q(x)に通し署名関数Q(β)を作り相手側に送り、相手側においてパラメータβから署名関数$Q^x(\beta)$を作成し、この署名関数

$Q^*(\beta)$と前記署名関数$Q(\beta)$とが一致したときのみデイジタル署名が行われたことを認証し、前記パラメータ$\beta$と署名関数$Q(\beta)$を格納エリア内に格納することを特徴とするICカードによる個人の認識方法。

**発明の詳細な説明**

〔発明の技術分野〕

この発明は、個人が通信回線を介して金融機関にアクセスする際に行うデータの暗号化と、デイジタル署名を行うことができるICカードによる個人の認証方法に関するものである。

〔従来の技術〕

従来、個人が金融機関の口座にアクセスする際、自身の身分証明には、自らのIDコードの書かれた磁気ストライプカードを用いていた。すなわち、第1図に示すように、口座にアクセスしようとする個人は、キャツシュデイスペンサ（ATMマシーン）1に磁気ストライプカード2を挿入し、暗証番号Aを投入して自らのIDコードを回線3を介して銀行4に送つていた。

しかし、この方法では、①回線3上のIDコードの盗読、②磁気ストライプカード2の偽造等が容易であるため、真の個人認識ができなかつた。また、磁気ストライプカード2では、信頼性のある署名の実現は困難であつた。なお、本明細書で用いる署名とは、個人が認識したことを相手側がいつでも確認できるようにすることをいう。

そこで最近では、第2図のようにキャツシュデイスペンサ（ATMマシーン）1と回線3の間に、専用の暗号装置（DES法、RSA法等を使用）5を置く方法が考えられている。しかし、この方法では、高価な暗号装置5が端末ごとに必要となる。また、DES法の場合、デイジタル署名の困難さ、金融機関による鍵管理の複雑さの点で、また、RSA法の場合、処理の複雑さ、暗号文の長さの点で問題がある。

〔発明の概要〕

この発明は、これらの欠点を除去するため、磁気ストライプカードの代りにCPU等を備えたICカードを使用し、ICカードの中に暗号機能、デイジタル署名機能を持たせたものである。以下、図面を用いてこの発明を詳細に説明する。

〔発明の実施例〕

第3図はこの発明による暗号化の一実施例を示すブロック図、第4図は処理の概要を示す処理説明図であり、第3図はICカード6がキャツシュデイスペンサ（ATMマシーン）1に挿入された状態を示す。



ICカード6は、その内部にCPU7とメモリ8を有している。メモリ8中には、暗号化鍵をなす暗号化関数F(x, y)や、個人IDおよびカード番号Nが格納されており、CPU7により鍵を掛けられている。鍵をオープンするためには、パスワードの投入が必要なようにICカード6内のアルゴリズムを設定しておく。このため、ICカード6の偽造は困難となる。

実際の処理は、第4図のようにして行う。

すなわち、ICカード6は、まず、自身のカード番号Nを銀行4に送る。これを受信した銀行4は、秘密のIDコード発生機関G(x)によりID′を計算する。次に、銀行4はICカード6に、乱数発生器等を使用して発生させたパラメータ$\alpha$を送る。これを受信したICカード6は、パラメータ$\alpha$と自身を有するIDを、暗号化関数F(x, y)に通し、暗号文F(ID, $\alpha$)を生成して銀行4に送る。ここに、ICカード6内に格納されたICは、カード製造時に秘密のIDコード発生関数G(x)とカード番号Nにより生成されたものである。暗号文F(ID, $\alpha$)を受信した銀行4は、復号化鍵をなす秘密関数$F^{-1}$(x, y)よりIDを計算する。そして、ID=ID′の場合のみ取引を許可する。すなわち、取引の許可を受けるのは、暗号化関数F(x, y)、秘密コードIDを有するカード（すなわち、銀行4が製造した正規のカード）のみということになる。

この方式においては、暗号化関数F(x, y)，IDの格納エリアのセキュリテイ、秘密関数$F^{-1}$(x, y)，IDコード発生関数G(x)の格納エリアのセキュリテイが大切となるが、前者は、ICカード6のメモリ8に対してCPU7により設けられる電子鍵、後者は銀行4のセンタの有するセキュリテイ機能により保護される。

次に、第5図のブロック図および第6図の処理説明図により、ICカード6が行うデイジタル署名の手順を説明する。なお、ICカード6には、署名関数Q(x)と、カード番号Nが格納されている。

ICカード6は、自らのカード番号Nを銀行4

に送る。銀行4は、カード番号Nを署名関数の発生関数P(x, y)にかけ、署名関数$Q^*(x)$の生成する。また、銀行4はパラメータβをICカード6に送る。ICカード6は受信したパラメータβを署名関数Q(x)に通し、署名関数Q(β)を作り銀行4に送る。銀行4は、パラメータβを用いて自らが作成した署名関数$Q^*(\beta)$とICカード6から送られてきた署名関数Q(β)を比較し、一致したときのみ署名されたと認証する。この時、パラメータβと署名関数Q(β)を自らの格納エリアに格納する。すなわち、パラメータβと署名関数Q(β)は、後で取引の事実を証明するデイジタル署名となり、銀行4はいつまでも確認を取ることができる。ここで、署名関数Q(x)、署名関数の発生関数P(x, y)は、それぞれICカード6，銀行4のセンタの安全エリアに格納される。

次に、上記デイジタル署名の有効性に付き考察する。

まず、パラメータβをランダムに生成すると、署名関数Q(β)の生成は署名関数Q(x)を有するICカード6（銀行4で発行したカード）にのみ可能となり、偽署名は困難となる。また、署名関数Q(x)はカード番号Nの関数であるため、この署名ができるのはそのカード番号Nを有するICカード6だけということになり、極めてセキュリティが高くなる。

なお、暗号化機能とデイジタル署名機能を1枚のICカード6内にインプリメントできるのはもちろんである。さらに、各関数は、カード内処理が容易なものを採用することができる。

〔発明の効果〕

以上説明したように、この発明では、暗号化および署名に必要なプロトコルをICカード内に有



しており、その格納領域は、ICカード内CPUにより保護されている。さらに、銀行等の相手側はIDコード発生関数、署名関数の発生関数、復号化鍵を有し、相手側からICカード側に乱数であるパラメータα，βを送つてICカード側で暗証文F(ID, α)や署名関数Q(β)を作成し、アクセスするたびにα，βを変えるようにしたので以下の利点を有する。

(1) ICカードの偽造が極めて難しい。

(2) 暗号化を行うため、真のIDは誰にも分らない。

(3) 暗号化、デイジタル署名に必要な処理が簡単である。

(4) ICカードごとに独自の暗号化、署名を行うため、そのセキュリテイは極めて高い。

(5) 銀行が行う関数、復号化鍵の管理が容易である。

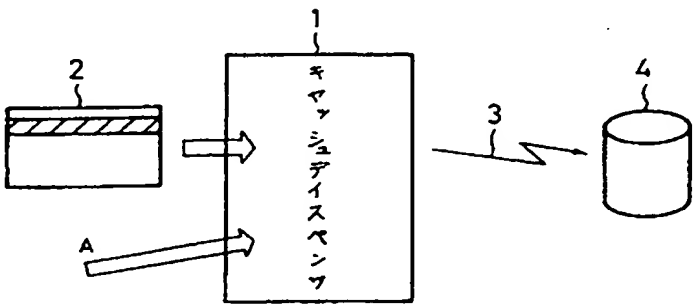
(6) ICカードのみで暗号化、署名を行うため、専用の暗号装置を用いる場合に比べて低格価である。

**図面の簡単な説明**

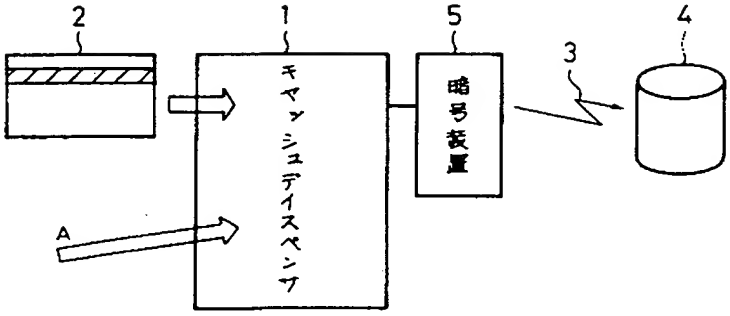
第1図は磁気ストライプカードを用いた銀行へのアクセス例を示す説明図、第2図は磁気ストライプカードと専用の暗号装置を用いたアクセス例を示す説明図、第3図はこの発明による暗号化の実施例を示す構成図、第4図はその処理説明図、第5図、第6図はこの発明によるデイジタル署名の実施例を示す構成図とその処理説明図である。

図中、1はキヤツシユデイスペンサ（ATMマシーン）、2は磁気ストライプカード、3は回線、4は銀行、6はICカード、7はCPU、8はメモリである。

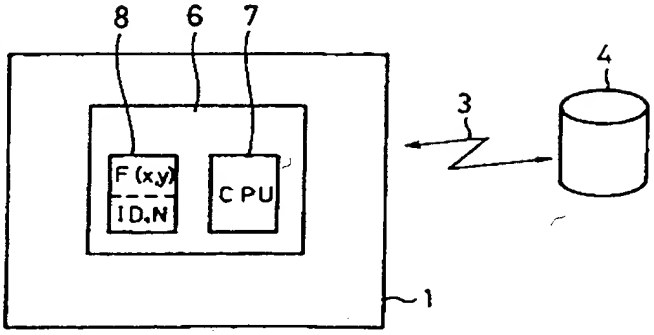
第1図



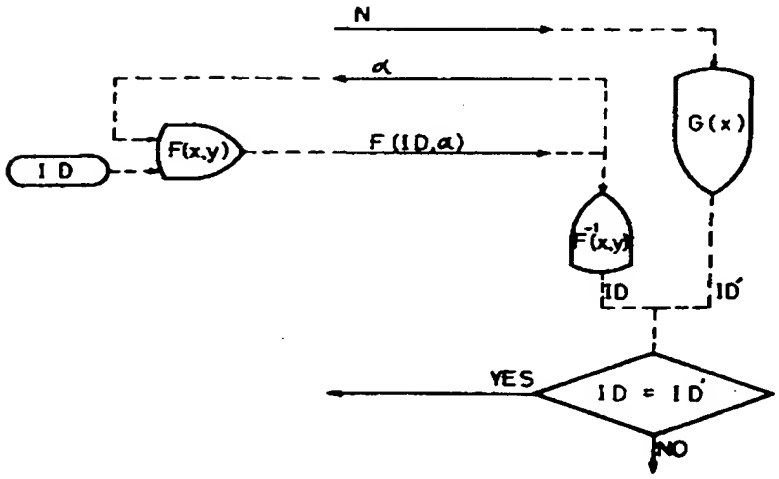
第２図


2
1
5
4
3
キャッシュディスペンサ
暗号装置
A

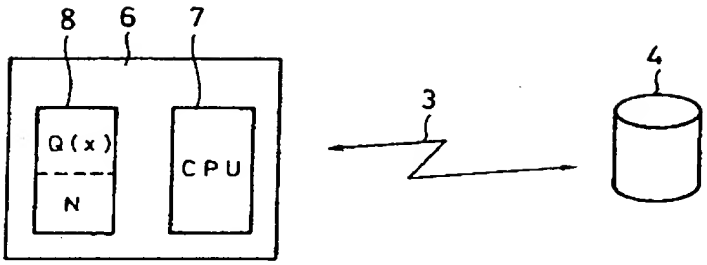
第３図


8
6
7
4
3
F(x,y)
ID,N
CPU
1

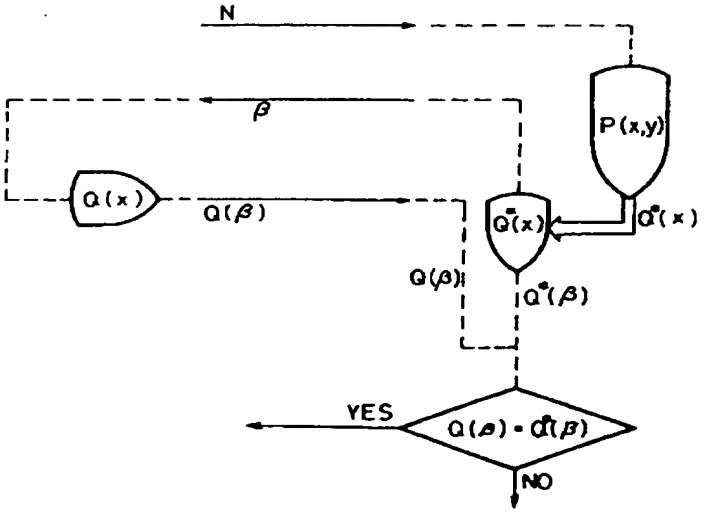
第４図


N
α
F(x,y)
F(ID,α)
ID
G(x)
F⁻¹(x,y)
ID
ID'
YES
ID = ID'
NO

第5図




第6図



【公報種別】特許法（平成６年法律第１１６号による改正前。）第６４条の規定による補正
【部門区分】第６部門第３区分
【発行日】平成８年（１９９６）１１月１３日

【公告番号】特公平５－６７９８０
【公告日】平成５年（１９９３）９月２８日
【年通号数】特許公報５－１７００
【出願番号】特願昭５９－１２５０
【特許番号】１９３９７２６
【国際特許分類第６版】
G06F 19/00
G06K 17/00 S 7623-5B
G07F 7/12
G09C 1/00 7259-5J
【ＦＩ】
G06F 15/30 340 9168-5L
350 9168-5L
G07F 7/08 B 330-3E

【手続補正書】
１　「特許請求の範囲」の項を「１　個人が秘密保護を必要とするデータを暗号化してオンラインで相手側に送信する場合において、暗号化関数とＩＤコードとカード番号をＩＣカード内のメモリにあらかじめ格納しておき、一方、ＩＤコード発生関数と復号化関数を相手側のセンタ内に設けておき、前記ＩＣカードから前記カード番号が入力されたときこのカード番号を前記ＩＤコード発生関数に通すことによりＩＤ′を算出し、一方、乱数であるパラメータαを前記ＩＣカードへ送り、前記ＩＣカードにおいて前記ＩＤコードと前記パラメータαとから前記暗号化関数によって暗号文Ｆ（ＩＤ，α）を生成して前記相手側に送り、この相手側において前記暗号文Ｆ（ＩＤ，α）を前記復号化関数に通してＩＤを算出し、前記ＩＤ′と前記ＩＤとが一致したときのみ前記個人の認証を行うことを特徴とするＩＣカードによる個人の認証方法。
２　個人が秘密保護を必要とするデータを暗号化してオンラインで相手側に送信し、相手が認証した後においてディジタル署名を行う場合において、暗号化関数、ＩＤコード、カード番号および署名関数Ｑ（ｘ）をＩＣカード内のメモリにあらかじめ格納しておき、一方、ＩＤコード発生関数、復合化関数および署名関数の発生関数Ｐ（ｘ，ｙ）を相手側のセンタ内に設けておき、前記ＩＣカードから前記カード番号が入力されたときこのカード番号を前記ＩＤコード発生関数に通すことによりＩＤ′を算出し、一方、乱数であるパラメータαを前記ＩＣカードへ送り、前記ＩＣカードにおいて前記ＩＤコードと前記パラメータαとから前記暗号化関数によって暗号文Ｆ（ＩＤ，α）を生成して前記相手側に送り、この相手側において前記暗号文Ｆ（ＩＤ，α）を前記復号化関数に通してＩＤを算出し、前記ＩＤ′と前記ＩＤとが一致したときのみ前記個人の認証を行い、その後のディジタル署名に際し、前記ＩＣカードから前記カード番号を相手側に送り、相手側において前記カード番号を前記署名関数の発生関数Ｐ（ｘ，ｙ）に通して署名関数Ｑ*（ｘ）を作成し、一方、乱数であるパラメータβを前記ＩＣカードに送り、前記ＩＣカード側は前記パラメータβを前記署名関数Ｑ（ｘ）に通し署名関数Ｑ（β）を作り相手側に送り、相手側において前記パラメータβから署名関数Ｑ*（β）を作成し、この署名関数Ｑ*（β）と前記署名関数Ｑ（β）とが一致したときのみディジタル署名が行われたことを認証し、前記パラメータβと前記署名関数Ｑ（β）を格納エリア内に格納することを特徴とするＩＣカードによる個人の認証方法。」と補正する。